Some Details on the Proof of VI (5.1)

This handouts provides more details on a part of the proof of VI Prop. 5.1.

In this handout, p will always refer to prime numbers.

Proposition VI 5.1. *Let* $\Omega = \prod_p \mathbb{Q}(\mu_{p^\infty})$ *(here the product symbol denotes the compositum of fields), let* $G = \mathrm{Gal}(\Omega/\mathbb{Q})$*, let* T *be the torsion subgroup of* G*, and let* $\widetilde{\mathbb{Q}} = \Omega^T$ *be the fixed field of* T*. Then* $\mathrm{Gal}(\widetilde{\mathbb{Q}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}$*.*

Proof. As was noted in class,

$$G \cong (\mathbb{Z}/2\mathbb{Z}) \times \prod_{p \neq 2} (\mathbb{Z}/(p-1)\mathbb{Z}) \times \widehat{\mathbb{Z}} , \tag{*}$$

and therefore $\mathrm{Gal}(\widetilde{\mathbb{Q}}/\mathbb{Q}) \cong G/\overline{T}$, where $\overline{T}$ denotes the closure of T (in the topology on G induced by its definition as a Galois group).

For convenience of notation, we note that $\mathbb{Q}(\mu_{2p}) = \mathbb{Q}(\mu_p)$ for all odd primes p, so we have

$$\mathbb{Q}(\mu_4) \prod_{p \neq 2} \mathbb{Q}(\mu_p) = \prod_p \mathbb{Q}(\mu_{2p}) .$$

We now claim that, in the decomposition (*), the subgroup $\widehat{\mathbb{Z}}$ (i.e., $0 \times 0 \times \widehat{\mathbb{Z}}$) is closed, and its fixed field is $\prod_p \mathbb{Q}(\mu_{2p})$. For this, it suffices to show for all p that

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{2p})/\mathbb{Q}) \times \mathbb{Z}_p ,$$

and that the subgroup $\mathbb{Z}_p$ in the above decomposition is closed, with fixed field $\mathbb{Q}(\mu_{2p})$.

Indeed, we first consider the case $p \neq 2$. Then, for all $n > 0$ we have canonical subgroups $G_{p,n}$ and $G'_{p,n}$ of $(\mathbb{Z}/p^n\mathbb{Z})^*$ such that $(\mathbb{Z}/p^n\mathbb{Z})^* = G_{p,n} \times G'_{p,n}$, $|G_{p,n}| = p-1$, and $|G'_{p,n}| = p^{n-1}$. Indeed, $G_{p,n}$ and $G'_{p,n}$ are the prime-to-p and p-power order torsion subgroups of $(\mathbb{Z}/p^n\mathbb{Z})^*$, respectively (and are the unique subgroups of $(\mathbb{Z}/p^n\mathbb{Z})^*$ of the given orders). Moreover, for all $p \neq 2$ and all n, the canonical map $(\mathbb{Z}/p^{n+1}\mathbb{Z})^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$ maps $G_{p,n+1}$ onto $G_{p,n}$ and $G'_{p,n+1}$ onto $G'_{p,n}$. Therefore, in the isomorphism $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/(p-1)\mathbb{Z}) \times \mathbb{Z}_p$, the fixed field of the subgroup $0 \times \mathbb{Z}_p$ is the compositum of the fixed fields of the $G'_{p,n}$ (which are all $\mathbb{Q}(\mu_p)$), hence the subgroup $0 \times \mathbb{Z}_p$ is closed with fixed field $\mathbb{Q}(\mu_p)$.

The case $p = 2$ is similar, but messier. Again we have $\mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}) \cong \mathbb{Z}_2^*$. We claim that $\mathbb{Z}_2^* \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}_2$. Indeed, the 2-power torsion subgroup of $\mathbb{Z}_2^*$ contains ± 1, but it contains no other elements. This is because this subgroup is cyclic, so it suffices to show that there are no torsion elements of order 4. However, any element of order 4 in a field of characteristic zero must be a root of $x^2 + 1 = 0$, but this equation has no roots in $\mathbb{Z}/4\mathbb{Z}$, hence none in $\mathbb{Z}_2/4\mathbb{Z}_2$. The congruence then follows from (II Prop. 5.7), since $a = 2$ in that proposition.

Therefore, since $\mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}) \cong \mathbb{Z}_2^*$, and since $\mathrm{Gal}(\mathbb{Q}(\mu_4)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, the short exact sequence

$$0 \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}(\mu_4)) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_4)/\mathbb{Q}) \longrightarrow 1$$

splits. Thus $\mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}(\mu_4)) \cong \mathbb{Z}_2^*/\{\pm 1\} \cong \mathbb{Z}_2$. (Here the first isomorphism is canonical, but the second one is not.) Hence we have

$$\mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\mu_4)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}(\mu_4)) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}_2 \ ,$$

where the first isomorphism is canonical, the factor $\mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}(\mu_4))$ is a closed subgroup with fixed field $\mathbb{Q}(\mu_4)$, and the second isomorphism preserves the factors.

Thus, the claim is proved.

Let

$$\widehat{T} = (\mathbb{Z}/2\mathbb{Z}) \times \prod_{p \ne 2} (\mathbb{Z}/(p-1)\mathbb{Z}) \ .$$

Then $G \cong \widehat{T} \times \widehat{\mathbb{Z}}$, and we identify G with $\widehat{T} \times \widehat{\mathbb{Z}}$ via this isomorphism. It suffices to show that $\overline{T} = \widehat{T}$.

Since $\widehat{Z}$ is torsion free, we have $T \subseteq \widehat{T}$. Moreover, $\widehat{T}$ is closed, so $\overline{T} \subseteq \widehat{T}$. Since T contains the subgroup

$$T' := (\mathbb{Z}/2\mathbb{Z}) \times \bigoplus_{p \ne 2} (\mathbb{Z}/(p-1)\mathbb{Z}) \ ,$$

it suffices to show that T' is dense in $\widehat{T}$.

This amounts to showing that, for all $x \in \widehat{T}$ and all closed subgroups $H < G$ of finite index, there is an $x' \in T'$ such that $x - x' \in H$.

By the claim, the fixed field of $\widehat{\mathbb{Z}}$ (under the isomorphism $G \cong \widehat{T} \times \widehat{\mathbb{Z}}$) is $\Sigma := \prod_p \mathbb{Q}(\mu_{2p})$, so $\mathrm{Gal}(\Sigma/\mathbb{Q}) \cong \widehat{T}$. Moreover, $\widehat{H} := H \cap \widehat{T}$ is closed of finite index in $\widehat{T}$, so it suffices to show that $x - x' \in \widehat{H}$ for some $x' \in T'$.

Let K be the fixed field of $\widehat{H}$ in Σ. Then K is finite over $\mathbb{Q}$, so there is a finite set P of primes such that $K \subseteq \prod_{p \in P} \mathbb{Q}(\mu_{2p})$.

Let $\widetilde{H} = \prod_{p \notin P} \mathrm{Gal}(\mathbb{Q}(\mu_{2p})/\mathbb{Q})$, regarded as a subgroup of $\prod_p \mathrm{Gal}(\mathbb{Q}(\mu_{2p})/\mathbb{Q})$ in the obvious way. Note that $\widetilde{H} \subseteq \widehat{H}$. For each prime p let x_p denote the component of x in $\mathrm{Gal}(\mathbb{Q}(\mu_{2p})/\mathbb{Q})$, and let $x' = \sum_{p \in P} x_p$. Then $x' \in \bigoplus_p \mathrm{Gal}(\mathbb{Q}(\mu_{2p})/\mathbb{Q}) = T'$, and

$$x - x' \in \prod_{p \notin P} \mathrm{Gal}(\mathbb{Q}(\mu_{2p})/\mathbb{Q}) = \widetilde{H} \subseteq \widehat{H} \ ,$$

as was to be shown. $\square$